Symantec.

It's time to wake up and smell the Virtsec Gravy!

John Reeman

1

Disclaimer

Please note that any views or opinions presented in this presentation are solely my own and do not necessarily represent those of my employer.

Nostalgia

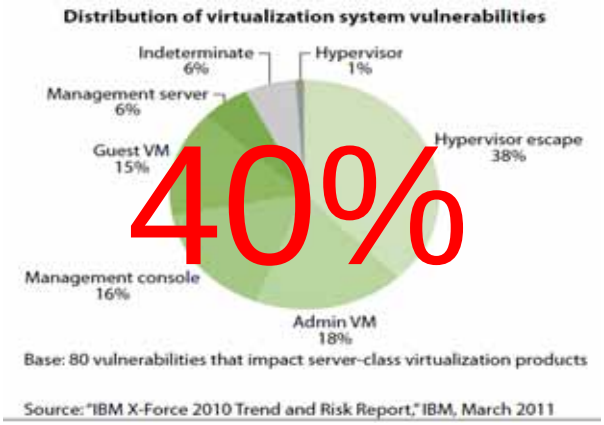
Techno magic....It just works!!!

Virtualization and Cloud

Do we believe virtualization...

- Is more secure, less secure, or the same?
- Gartner has told us that through 2012, “60% of virtualized servers will be less secure than the physical servers they replace”
- A recent CSO flash poll conducted by Symantec revealed that while 70% of respondents reported that security and compliance concerns have not slowed the pace of adoption in their organizations, 75% indicated that security and compliance are the largest factors in keeping them from full confidence when it comes to hosting business critical applications on virtualized servers.

Some interesting stats...



"Looking deeper into hacking activity, it is apparent that the bulk of attacks continues to target applications and services rather than the operating systems or platforms on which they run." - Verizon Report

10

Real World Examples

Admin hacks drug company virtual machines from McDonald's

Logging in from a McDonald's restaurant, a former employee of a US pharmaceutical company was able to wipe out most of the company's computer infrastructure earlier this year. Jason Cornish, 37, formerly an IT staffer at a subsidiary of Japanese drug maker Shionogi, pleaded guilty to computer intrusion charges in connection with the attack on February 3, 2011. He wiped out 15 VMware host systems that were running email, order tracking, financial and other services for the company.

"The attack effectively froze Shionogi's operations for a number of days, leaving company employees unable to ship product, to cut checks, or even to communicate via email," the Department of Justice said in court filings. Total cost to Shionogi was around $800,000 (£488,000).

11

More Real world examples

- Salesforce.com - Clickjacking 2009

Source Sensepost (www.sensepost.com/blog/3741.html)

- Amazon outages - April 26th 2011

Source CSO Online (www.csoonline.com/article/680894/amazon-outage-a-valuable-lesson-in-cloud-security)

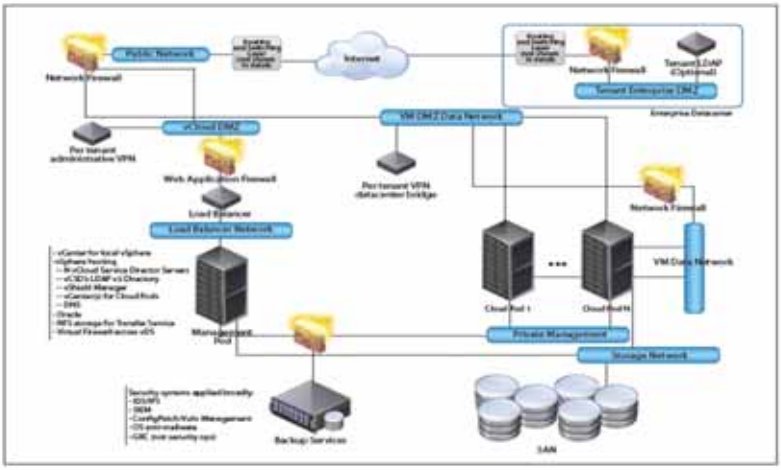
- Continued persistent threats from individuals and groups is a given
- Anonymous Source code leakage ! April 24th VMware

Source The Inquirer (www.theinquirer.net/inquirer/news/2170503/hardcore-charlie-disputes-downplaying-vmware-code)

FUD

Simple but effective attack

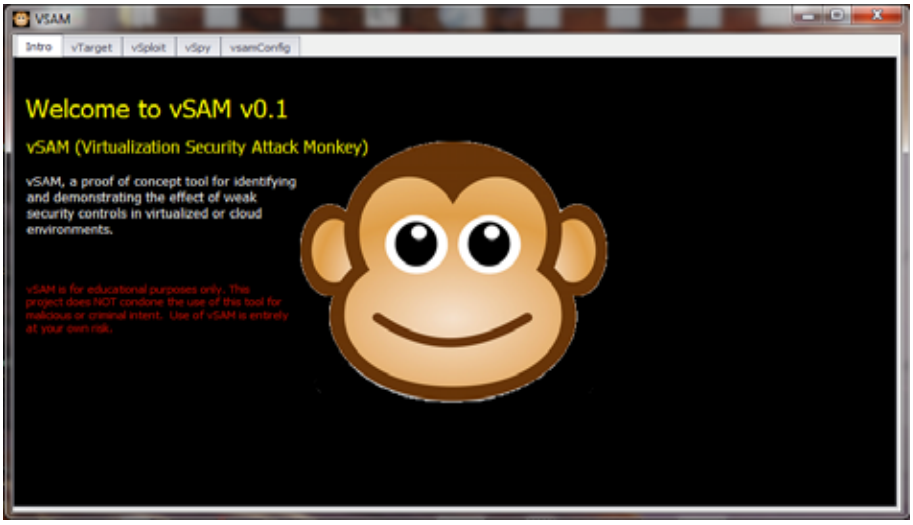
One example – what's wrong?



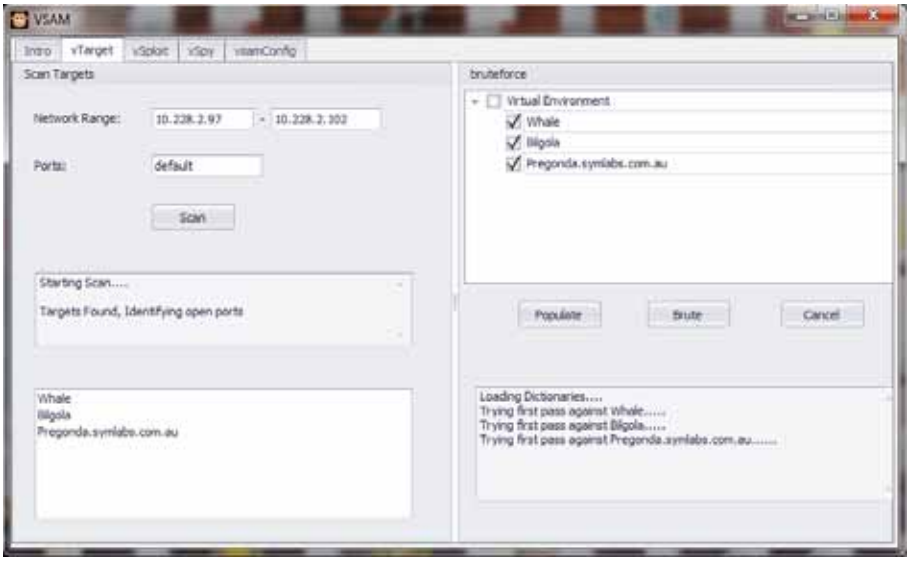
Under the hood....

- My research over the years has involved doing binary analysis of code as well as reversing
- Strings analysis
- Looking for hidden hooks in api's
- To try and discover 0 days
- But what I am about to show you is much simpler than that....

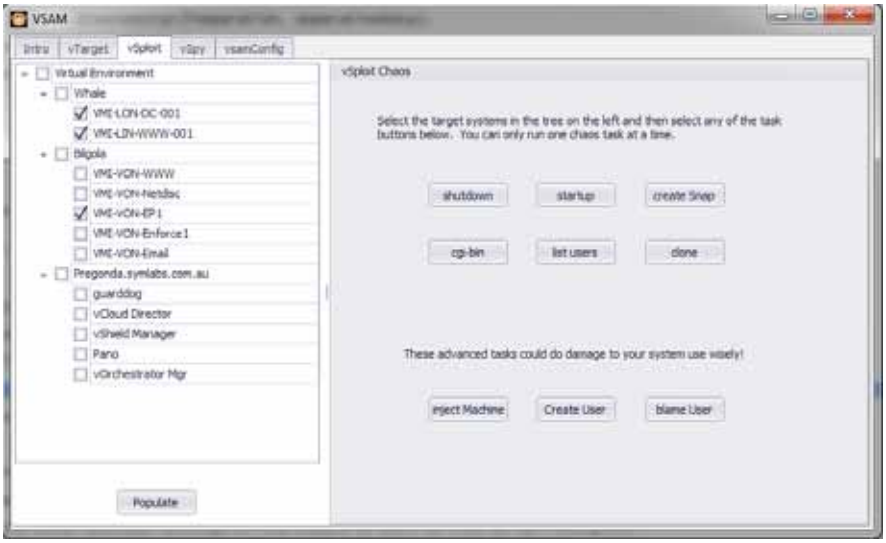
Introducing VSAM



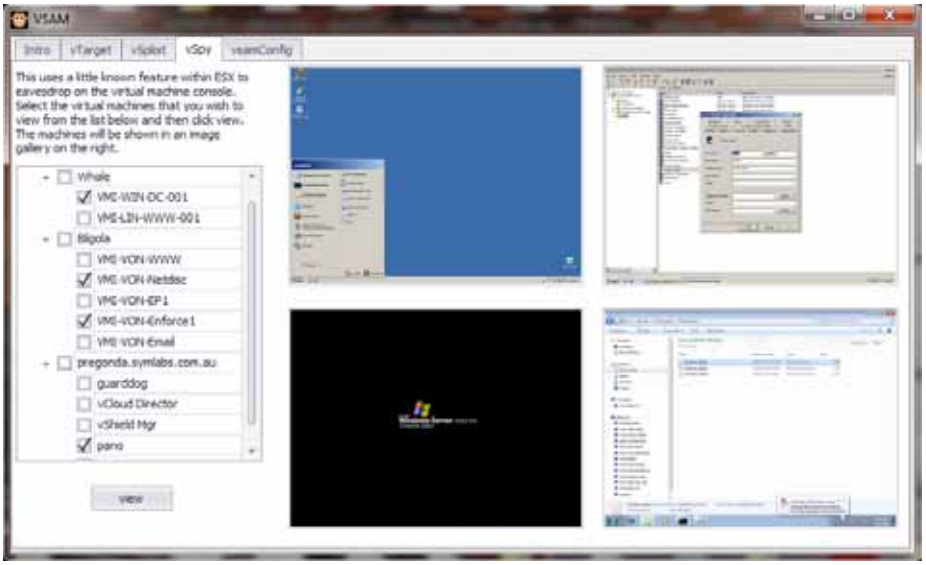
Identify our target



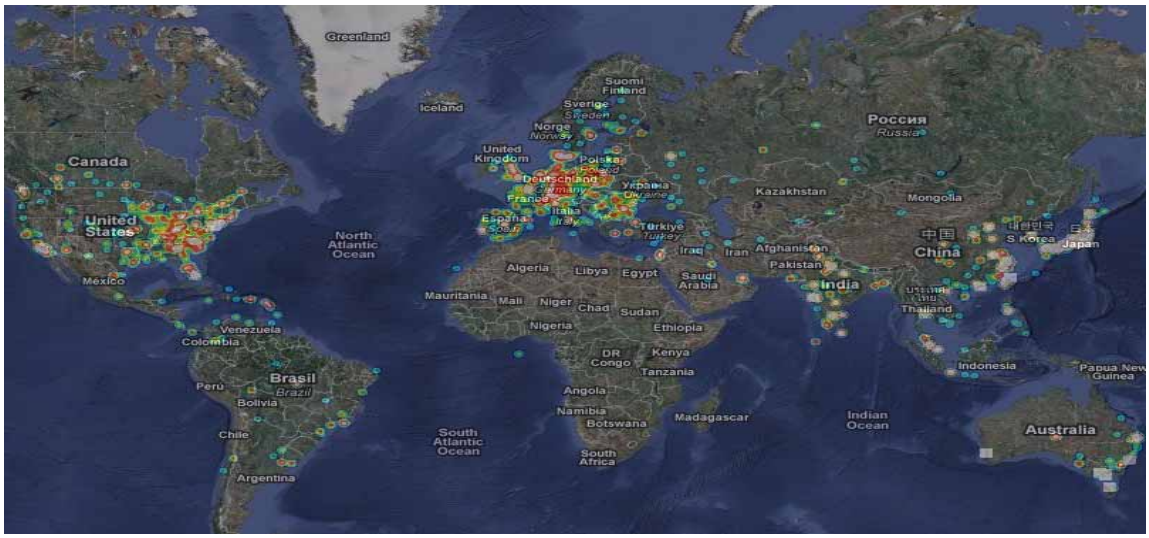
chaos and fun



Looking over your shoulder...



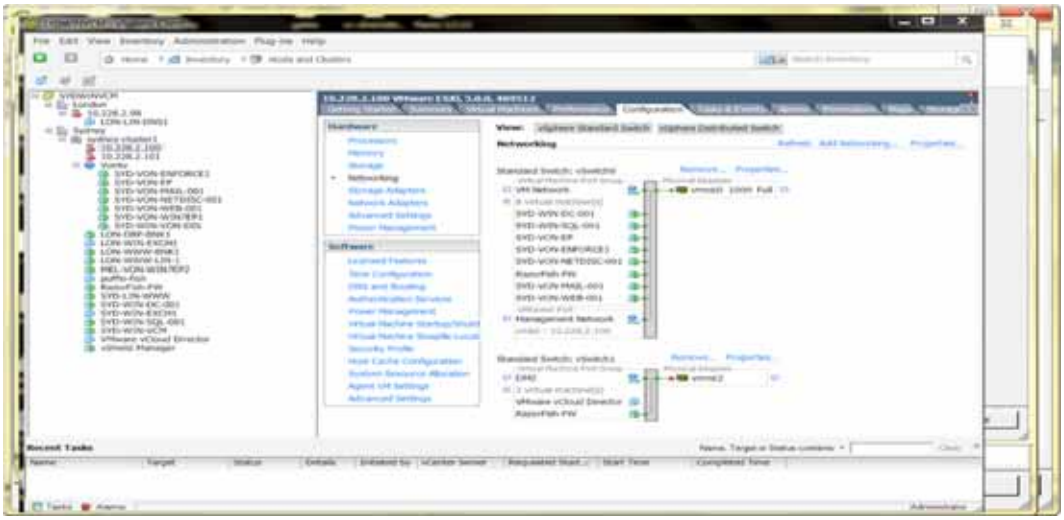
Targeted attacks



We need to get better...

- Patching - yes it's a chore but there's no excuse anymore! (the vendors do their part so it's up to us)
- DSD Top 35
- Go back to basics; it's not all about technology
- Both Virtualization and Cloud Technology introduce new dynamics involving the network, storage and applications
- Data privacy issues exist, cross borders etc
- BUT if we are to embrace Cloud & Virtualization it is essential that we secure access to the API's or at least reduce risk

5 Mouse Clicks to build a network!



23

crossroads of past and future...

A new approach....

- Traditional security methods and even some virtualization security approaches are not adequate...
- We need to go beyond Firewalls; there are no boundaries remember...
- WAFs are not the answer....
- There is a need for an independent multilayered approach that involves the business and technology

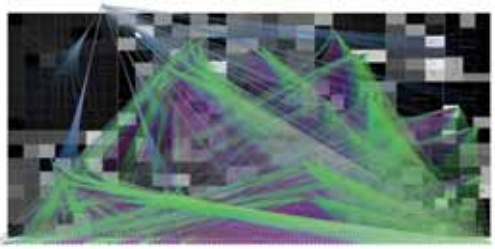
In the future...

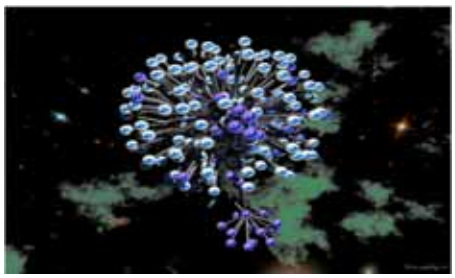
- Innovate to get better
- Advanced dynamic threat protection
- We live in a world now that is no longer IP centric but is more about objects, resources, assets, applications, services, the digital native
- We are dealing with large data sets that the human brain cannot comprehend
- We need to leverage other technology from both the past and future...

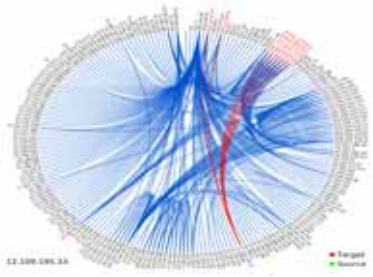
From the worlds of....

Helping to Make sense of BIG DATA

Security Visualization







Secure bubbles....

Closing thoughts....

- We can do this....
- The expertise is there
- We have some cool technology out there
- We can leverage from history
- But some of it will involve going back to basics! (patching, hardening etc)
- Need for an effective risk management strategy
- We need a skilled workforce that understands...
- It's not just about 5 clicks of a mouse....

Thanks for listening

Want to know more then:-

@spiv
John_Reeman@symantec.com
+61 418 911 474

27